REMARKS

The application has been reviewed in light of the Office Action dated March 8, 2004. Claims 1-24 are pending in this application, with claims 1, 6, 11 and 16 being in independent form. Claims 1, 6-7, 11, and 16 have been amended to correct formal matters not effecting the scope of the claims. Claims 21-24 have been added. It is respectfully submitted that no new matter has been added and no new issues have been raised by the present response.

Claims 1-20 were rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite. Without conceding the propriety of this rejection, the claims have been carefully reviewed and amended to expedite examination of the application. The changes being made are believed formal in nature and are not intended to alter the scope of the claims.

Claims 1-2, 5-7, 10-12, 15-17, and 20 were rejected under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. Patent 6,067,410 to Nachenberg. Claims 3, 8, 13, and 18 were rejected under U.S.C. § 103(a) as allegedly unpatentable over Nachenberg, in view of U.S. Patent No. 6,401,210 to Templeton. Claims 4, 9, 14, and 19 were rejected under U.S.C. § 103(a) as allegedly unpatentable over Nachenberg, in view of Internet Article XP002201936, AntiVirus Research Center, "Happy99.Worm Removal Tool" (hereinafter "Happy99").

Applicants have carefully considered the comments in the Office Action and the cited art, and respectfully submit independent claims 1, 6, 11 and 16 are patentable over the cited art for at least the following reasons.

Independent claim 1 relates to a method for restoring a computer system modified by malicious code, comprising scanning the computer system for the malicious code, identifying the malicious code, retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to

modification by the malicious code, and executing the at least one command to restore the computer system to the state as it existed prior to modification by the malicious code.

Nachenberg, as understood by Applicants, relates to an emulation repair system that restores virus-infected computer files to their uninfected states without infecting the rest of the computer system. The system includes a virtual machine for emulating the virus-infected computer file, a foundation module including generic, machine language repair routines, and a virus specific overlay module. The emulation repair system receives the identity of the infected computer file and the infecting virus from a virus scanning module, and uses the received information to access a virus definition that includes decryption information on the identified virus. The infected computer file is emulated in the virtual machine until it is determined from comparison with the decryption information that the virus is fully decrypted. The foundation and overlay modules are then loaded into the virtual machine and control of the virtual machine is given to the overlay module. The overlay module calls repair routines in the foundation module, the overlay module, and the virus itself, as necessary, to restore over-written host bytes from the infected host file to their proper locations in the infected host file.

As understood by Applicants, col. 8, lns. 20-31 of Nachenberg describes a virus definition file. The virus definition file includes data fields including an identification data field ("VirusID"), a virus signature data field ("SigStart" and "SigEnd"), a data field specifying a maximum number of instructions needed to decrypt the virus ("VirusExecutionCap"), and a data field specifying a maximum number of instructions that must be emulated to repair a host file ("RepairExecutionCap") (see Nachenberg, col. 8, lns. 34-60). Other parameters associated with a virus may be specified using a "Flags" field, and the data field "RepairFile" is used to specify a binary filename of an associated overlay program (see id., col. 8, lns. 61-67).

Accordingly, Nachenberg is concerned with restoration of virus-infected computer files.

In contrast, the present independent claims are directed to restoring the computer system to a state that existed prior to modification by malicious code. Accordingly, Applicants find no teaching or suggestion in the cited art of retrieving from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code, as recited in amended independent claim 1.

Accordingly, Applicants submit independent claim 1 is patentably distinct from the cited art. Independent claims 6, 11, and 16 are believed to be patentably distinct from the cited art for at least similar reasons.

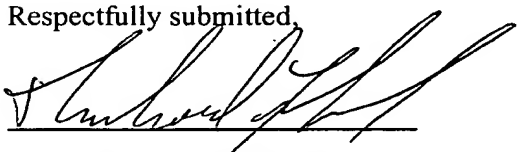
The Office is hereby authorized to charge any additional fees that may be required in connection with this response and to credit any overpayment to our Deposit Account No. 03-3125.

If an additional petition for extension of time is required to make this response timely, this paper should be considered to be such a petition, and the commissioner is authorized to charge the requisite fees to our Deposit Account No. 03-3125.

If a telephone interview could advance the prosecution of this application, the Examiner is respectfully requested to call the undersigned attorney.

Entry of this response and allowance of the present application are respectfully requested.

Respectfully submitted,



RICHARD F. JAWORSKI
Reg. No. 33,515
Attorney for Applicants
Cooper & Dunham LLP
Tel.: (212) 278-0400